# SECUREDATA, Inc.
# SecureUSB KP

FIPS 140-2 Non-Proprietary Security Policy
Version 1.0

# Table of Contents

# List of Tables



# List of Figures

# 1 Cryptographic Module Specification

## 1.1 Overview

The SECUREDATA, Inc. SecureUSB KP is a multi-chip, stand-alone, cryptographic module that provides hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated with user input via the built-in keypad. User data is protected by 256-bit XTS-AES encryption that secures sensitive information from unauthorized disclosure in the event that the module is lost or stolen. The custom electronics within the module are encapsulated within an opaque, production grade epoxy. There is a non-replaceable battery within the module. The module's enclosure defines the cryptographic boundary[1].

The data encryption key (DEK) and other critical security parameters (CSPs) are generated by a NIST approved DRBG[2] within the module when it is first used. The seed for the DRBG is also produced within the module from a hardware-based, entropy generator.

The user interface for the module is an alphanumeric keypad with eleven (11) buttons and three (3) status-indicator LEDs. The LEDs are each a different color, red green and blue, and in distinct locations. The keypad accepts the User or CO PIN/Password when creating new credentials and when authenticating to unlock the module. The LEDs provide status information while entering authentication credentials and using the module.

1 Excluded components within the cryptographic boundary include passive electronic components, LEDs, and a rechargeable battery.

2 *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).

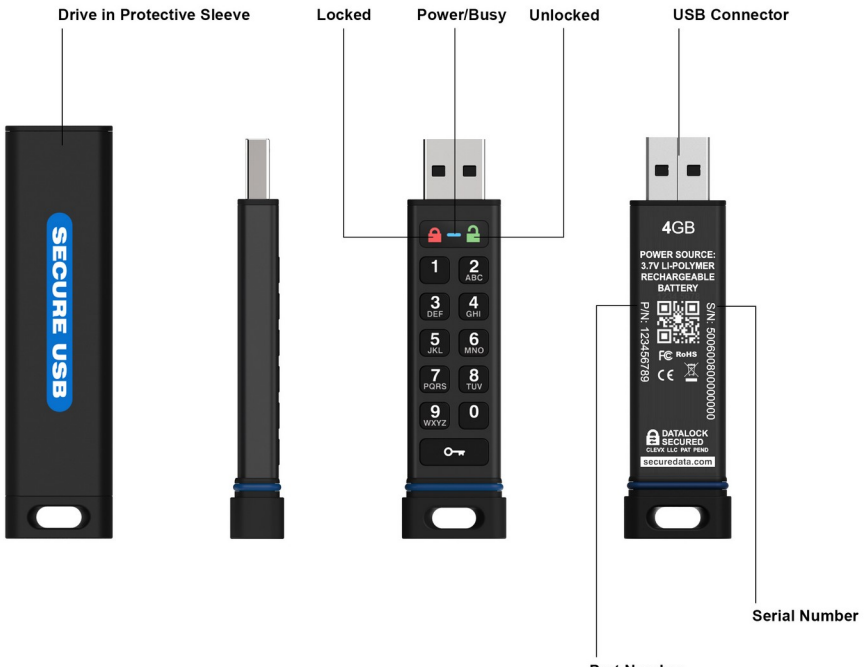


*Figure 1: SecureUSB KP*

| Hardware Part Numbers | Firmware Versions |
|---|---|
| SU-KP-BL-4<br>SU-KP-BL-8<br>SU-KP-BL-16<br>SU-KP-BL-32<br>SU-KP-BL-64 | Each module has one each of Firmware A and Firmware B.<br><br>*Firmware A*<br>V1.01.10<br><br>*Firmware B*<br>V1.11.1 or V1.12<br>(no security relevant differences) |

*Table 1: Module Hardware and Firmware Versions*

## 1.2 FIPS Security Level

The module meets the overall requirements for FIPS 140-2[3] Level 3.

| FIPS Area | FIPS Security Requirement | Level |
|---|---|---|
| 1 | Cryptographic Module Specification | 3 |
| 2 | Module Ports and Interfaces | 3 |
| 3 | Rôles, Services, and Authentication | 3 |
| 4 | Finite State Model | 3 |
| 5 | Physical Security | 3 |
| 6 | Operational Environment | *n/a* |
| 7 | Cryptographic Key Management | 3 |
| 8 | EMI/EMC | 3 |
| 9 | Self-Tests | 3 |
| 10 | Design Assurance | 3 |
| 11 | Mitigation of Other Attacks | *n/a* |

*Table 2: FIPS Security Level*

3 *FIPS 140-2 – Security Requirements for Cryptographic Modules*. NIST. (December 2002).

## 1.3 Mode of Operation

The module operates only in a FIPS approved mode. This approved mode, where firmware integrity checks and KATs completed successfully, is identified by the three status-indicator LEDs blinking once simultaneously when the module is powered on.

To meet the requirements for FIPS 140-2 Level 3, the module enforces the following security rules:

- The cryptographic module provides two distinct operator rôles: User and Cryptographic Officer (CO).
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid rôle or is in an error state, the operator shall not have access to any cryptographic service.
- The operator is capable of commanding the module to perform self-tests at any time by cycling the power.
- Data output is inhibited during self-test, zeroization, key generation, and authentication.
- No CSPs are output from the module in any form.

# 2 Module Ports and Interfaces

The cryptographic module exposes the following physical ports and logical interfaces:

| Physical Port | Logical Interface | Description |
|---|---|---|
| USB Data | Data input<br>Data output<br>Control input<br>Status output | The USB Data port connects the module to the host computer. It is used to exchange decrypted user data as well as control and status information for the USB protocol. When the drive is locked the USB interface is disabled. |
| Alphanumeric Keypad (0-9) | Data input | The keypad with ten (10) alphanumeric labeled buttons is connected to button inputs. The keypad is used to enter User or CO PIN/Password. |
| KEY button | Control input | The **KEY** button is connected to a button input. It is used to awaken the module from low-power sleep and to control UI flow including selection of the rôle. |
| Red, green and blue LEDs | Status output | Refer to Table 4 for details. |
| USB Power | External power | The USB VBUS (+5VDC) charges the battery and powers the module and embedded storage component. |

*Table 3: Module Ports and Interfaces*

| LED Behavior | Module State | Status Description |
|---|---|---|
| All three LEDs blink once simultaneously | Connected to USB power | Module powered-on with all LEDs operational. Firmware integrity tests and KATs have passed. |
| No LEDs illuminate on pressing the **KEY** button when the module is powered off. | Disconnected | The battery is most likely fully discharged in which case it must be charged for at least one minute before powering on the module.. If the module fails the firmware integrity test, the LEDs will not illuminate. |
| LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily. | Failed | Module in error state. |
| Red LED blinking | Locked | Waiting for User PIN/Password to unlock |
| Red and blue LEDs blinking | Locked | Waiting for User PIN/Password to unlock. CO PIN/Password is set. |
| Red LED on solidly | Locked | Module verifying User PIN/Password |
| Green LED on solidly | Disconnected | Unlocked and ready to connect to PC |
| Green LED on solidly and blue LED blinking | Connected | Unlocked, connected to PC via USB, and communicating or transferring data |
| Green and blue LEDs on solidly | Connected | Unlocked and connected to PC via USB |
| Green LED on with single blink every 2 seconds and blue LED blinking | Connected | Unlocked, connected to PC via USB, and communicating or transferring data. Drive configured in read-only mode |
| Green LED on with single blink every 2 seconds and blue LEDs on solidly | Connected | Unlocked and connected to PC via USB. Drive configured in read-only mode. |
| Red LED blinking and green LED on solidly. | UI | User authenticated and module configuration UI is active. |
| Red LED blinking and green LED blinking quickly. | UI | CO authenticated and module configuration UI is active. |
| Red LED blinks very slowly. | Locked and disconnected | Module is awake and there is neither User nor CO PIN/Password defined after reset. |
| Blue LED blinking | Disconnected | Ready to accept new User PIN/Password |
| Green LED blinking after entering new User/CO PIN/Password | Disconnected | Ready to accept new PIN/Password a second time as confirmation |
| Red and blue LEDs blinking | Disconnected | Ready to accept new CO PIN/Password |
| Red and green LEDs blinking | Locked | Waiting for CO PIN to unlock. User PIN/Password is set. |
| Blue LED blinking | Locked | No User PIN/Password |
| Red and green LEDs blinking alternately | Disconnected | Factory reset initiated. Module waiting for confirmation code. |
| Red LED illuminates and then fades out and then illuminates solidly | Disconnected | Module locked and disconnected |
| Red LED illuminated. Blue LED blinking slowly. | Locked | Battery charging |

*Table 4: LED Status Indications*

To verify that the module is in good working order, power it on by connecting it to a USB power source. The three status indicator LEDs will blink once, simultaneously, indicating that firmware integrity tests and KATs have passed successfully.

# 3 Rôles, Services, Authentication, and Identification

## 3.1 Rôles and Identification

The module implements level 3, identity-based authentication with two distinct identities, one User identity and one Crypto-Officer identity.

| Identity | Identification | Authentication Data | Description |
|---|---|---|---|
| User[4] | Identifies as User by pressing **KEY** button | 7-15 digit PIN/Password | User has full access to all User services. |
| CO | Identifies as CO by pressing **1 button** and **KEY** button | 7-15 digit PIN/Password | CO has full access to all CO services. |

*Table 5: Module Rôles*

4 In the case where the User PIN is defined but no CO PIN is defined, the User identity behaves as a combined User/CO identity.

## 3.2 Module Initialization

A new module comes from the factory initialized with a default User PIN/Password of **`11223344`**. This factory default password must be changed before storing confidential data on the module[5]. No CO PIN/Password is defined for a factory initialized module. In the factory initialized configuration, the module is ready for operation in a FIPS approved mode.

If the module is zeroized, there will be neither a User PIN/Password nor a CO PIN/Password defined and there will be no DEK. The module must be initialized before it will operate in an approved mode. From this state, either a User or a CO PIN/Password may be defined first.

5 Per FIPS 140-2 §4.3.3, the default password does not meet the strength of the authentication requirement because it may be guessed in one attempt.

## 3.3 Services

| Identity | Service | CSP Access |
|---|---|---|
| CO | Set CO PIN/Password | Read, Execute, and Write<br>Change CO PIN/Password, CO salt, and CO KEK.<br>Create DEK using CTR-DRBG state (seed, V, key) if one is not defined. |
| | Set User PIN/Password | Read, Execute, and Write<br>Change User PIN/Password, User salt, and User KEK. |
| | Zeroize User PIN/Password | Zeroize<br>Zeroize User salt and User KEK. |
| | Erase private partition data | Read, Execute, and Write<br>Change CO salt and CO KEK. Create DEK using CTR-DRBG state (seed, V, key).<br>Zeroize<br>Zeroize User salt and KEK. |
| | Open private partition for read/write access to user data | Read and Execute<br>Read CO salt and CO KEK. Unobfuscate DEK. |
| | Lock private partition to prevent read/write access to user data | Zeroize<br>Zeroize DEK in RAM. |
| | Read or write private partition with user data | Read and Execute<br>Use DEK to encrypt and decrypt user data. |
| | Configure idle timeout lock | None |
| User | Set CO PIN/Password when none exists | Read, Execute, and Write<br>Change CO PIN/Password, CO salt, and CO KEK. |
| | Set User PIN/Password | Read, Use, and Write<br>Change User PIN/Password, User salt, and User KEK.<br>Create DEK using CTR-DRBG state (seed, V, key) if one is not defined. |
| | Open private partition for read/write access to user data | Read and Execute<br>Read CO salt and CO KEK. Unobfuscate DEK. |
| | Lock private partition to prevent read/write access to user data | Zeroize<br>Zeroize DEK in RAM. |
| | Read or write private partition with user data | Read and Execute<br>Use DEK to encrypt and decrypt user data. |
| | Configure idle timeout lock | None |

| Identity | Service | CSP Access |
|---|---|---|
| Unauthenticated | Show locked/unlocked status | None |
| | Show whether or not drive is initialized | Read and Execute<br>Verify validity of either User salt or CO salt. |
| | Show whether or not User PIN/Password is defined | Read and Execute<br>Verify validity of User salt. |
| | Show whether or not CO PIN/Password is defined | Read and Execute<br>Verify validity of CO salt. |
| | Run self-tests | None |
| | Factory reset (zeroize) module and erase private partition data | Zeroize<br>Zeroize all CSPs. |

*Table 6: Services Available in FIPS Approved Mode*

## 3.4 Authentication

The Crypto Officer and User rôles authenticate via the module's keypad interface. The module does not output CO or User authentication data outside of the cryptographic boundary.

The PIN/Password, from either the User or the CO, is an input to PBKDFv2 that produces the Key Encryption Key (KEK) for that rôle. The KEK is used by the non-approved cryptographic Synthetic Initialization Vector[6] (SIV) algorithm to obfuscate the DEK. SIV is constructed using AES CTR (Cert. #C 78) and AES CMAC (Cert. #C 78). Unobfuscating the DEK requires the same PIN/Password that was given to PBKDFv2 when the DEK was obfuscated.

The authentication strength for the module is determined by the PIN/Password. The PIN/Password is composed of a sequence of decimal digits 0-9, as marked on the keypad buttons, selected by the User or CO. Most of the buttons also bear alphabetic letters (see Figure 1). The minimum PIN/Password length is seven (7) digits. The maximum PIN/Password length is 15 digits. The probability of a successful, random guess of a minimum length PIN/Password is approximately $10^{-7}$ or 1 chance in 10,000,000[7].

The module protects against brute-force attempts to guess a rôle's PIN/Password by permitting no more than ten (10) consecutive incorrect guesses before locking out that rôle. Incorrect PIN/Password attempts are counted independently for each rôle. The probability of an attacker correctly guessing a PIN/Password in any time period[8], such as a one-minute interval, is $10^{-6}$ or 1 chance in 1,000,000.

---

6 Harkins, D. *Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)*. IETF. (October 2008)

7 Sequential and repeating PINs are not allowed. For example, the module will reject a PIN of 1-2-3-4-5-6-7 or 6-5-4-3-2-1-0. Attempts to create such a PIN will cause the module to indicate an error. There are 270 such combinations.

8 The FIPS 140-2 standard stipulates that "*For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 ($10^{-5}$) that a random attempt will succeed or a false acceptance will occur.* " In this product, a single successful attempt to guess a PIN/Password has a probability one in 10,000,000 ($10^{-7}$). Ten guesses has a probability of one in 1,000,000 ($10*10^{-7}$ or $10^{-6}$) of success. The standard requires that the probability of a successful guess be less than one in 100,000 ($10^{-5}$) in a one-minute period. The authentication mechanism of this module is better than the standard requires, over any time interval—including a one-minute period. A probability of one in 1,000,000 ($10^{-6}$) is less likely than one in 100,000 ($10^{-5}$).

# 4 Physical Security

The multi-chip standalone cryptographic module includes the following physical security mechanisms, conforming to FIPS 140-2 Level 3 requirements:

1. Production grade components
2. Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components. Epoxy hardness was tested at ambient temperature meaning that no assurance is provided for Level 3 hardness conformance at any other temperature.
3. Memory protection enabled to prevent read-out of firmware, RAM, or NVRAM

The operator is responsible for inspecting the module on each use for evidence of tampering. If the module is physically compromised it is no longer guaranteed to provide FIPS protections and should be replaced.

# 5 Operational Environment

The FIPS 140-2 Operational Environment (Area 6) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

# 6 Cryptographic Key Management

## 6.1 Cryptographic Algorithms

| Algorithm | Modes | Key Sizes | Reference | CAVP Cert. | Use |
|---|---|---|---|---|---|
| AES | XTS[9] | 256 | NIST SP 800-38E[10] | AES 5942 | Encryption of user data within storage application only |
| AES | ECB<br>CMAC<br>CTR | 128<br>256<br>(ECB & CTR only) | FIPS 197[11]<br>NIST SP 800-38A[12] | C 78 | Block cipher basis of CTR-DRBG and algorithmic basis for SIV |
| CKG | - | 256 | NIST SP-800-133[13] | Vendor Affirmed | The unmodified output of the DRBG is used for generating symmetric keys |
| DRBG | AES-CTR | 256 | NIST SP 800-90A[14] | C 78 | Random number generator for encryption keys and salts |
| HMAC | HMAC-SHA-1 | 160 | FIPS 198-1[15] | C 78 | Algorithmic basis of PBKDFv2 |
| PBKDFv2 | HMAC-SHA-1 | - | NIST SP 800-132[16] | Vendor Affirmed | KEK generation. Password is the same as the User/CO PIN/Password with a minimum length of 7 digits 0-9. Algorithm conforms to FIPS 140-2 Implementation Guidance (IG) D.6: the module supports option 2a as documented in SP 800-132 § 5.4. |
| SHS | SHA-1 | - | FIPS 180-4[17] | C 78 | Algorithmic basis of HMAC-SHA1 |

*Table 7: FIPS Approved Algorithms*

9 ECB modes is included in the CAVS certificate, but is used by no services in the module.
10 *SP 800-38E – Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. NIST. (January 2010).
11 *FIPS 197 – Advanced Encryption Standard (AES)*. NIST. (November 2001).
12 *SP 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST. (December 2001).
13 *SP 800-133 – Recommendation for Cryptographic Key Generation*. NIST. (December 2012).
14 *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).
15 *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. NIST. (July 2008).
16 *SP 800-132 – Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*. NIST. (December 2010).
17 *FIPS 180-4 – Secure Hash Standard (SHS)*. NIST. (August 2015).

| Algorithm | Strength | Use |
|---|---|---|
| NDRNG | Module generates cryptographic keys with a minimum security strength of 256 bits. | Entropy source for seed to CTR-DRBG |

*Table 8: FIPS Allowed Algorithms*

| Algorithm | Use |
|---|---|
| SIV[18] (no security claimed) | Per FIPS 140-2 IG §1.23, SIV is a non-approved cryptographic algorithm. It is allowed in FIPS approved mode. It is not a security function. *"Cryptographic keys and CSPs encrypted using a non-approved algorithm or proprietary algorithm or method are considered in plaintext form, within the scope of this standard [FIPS 140-2]."*<br><br>SIV is used during authentication and meets all authentication strength requirements. SIV uses the CO KEK and User KEK, derived from the CO or User PIN/Password via KBKDFv2, to obfuscate and unobfuscate the DEK. |

*Table 9: FIPS Non-approved Algorithms*

## 6.2 Critical Security Parameters

The module does not output or establish CSPs--either by key agreement or key transport. The only CSPs entered into the module are plaintext PIN/Passwords via the keypad. KEKs are derived using PBKDFv2[19] and are only used as part of the module's data storage application.

18 Harkins, D. Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). IETF. (October 2008). SIV is a Authenticated Encryption algorithm codified by the IETF in RFC-5297. NIST has not analyzed this algorithm, so it is specified here as non-approved for the purposes of FIPS 140-2. Obfuscation of the DEK depends on the user's PIN/Password and SIV to prevent the plaintext DEK from being stored in NVRAM. NIST characterizes the storage of the DEK as plaintext explicitly because SIV is non-approved.

19 Per FIPS SP800-132 and FIPS140IG § D.6, the materials derived from PBKDFv2 are used only for "protection of electronically-stored data or for the protection of data protection keys."

| Parameter | Description | Source | Storage | Creation / Destruction |
|---|---|---|---|---|
| CTR-DRBG state (seed, V, key) | Generating random values for CSPs<br><br>256 bit output (full entropy) | NDRNG and CTR-DRBG | RAM | Created when DRBG is seeded which is every time the module initializes |
| | | | | Destroyed on lock, connect, successful generation of CSPs, power-off, and zeroization |
| User PIN/Password | Input to PBKDFv2 to allow generation of the User KEK<br><br>Strength of 7-15 digits | Keypad entry | RAM | Created by User |
| | | | | Destroyed on lock, unlock, timeout, power-off |
| CO PIN/Password | Input to PBKDFv2 to allow generation of the CO KEK<br><br>Strength of 7-15 digits | Keypad Entry | RAM | Created by CO |
| | | | | Destroyed on lock, unlock, timeout, power-off |
| User Salt | Input to PBKDFv2 to generate key to obfuscate DEK<br><br>128 bit value | CTR-DRBG | NVRAM | Created when User changes PIN/Password |
| | | | | Destroyed on PIN/Password change, zeroization |
| CO Salt | Input to PBKDFv2 to generate key to obfuscate DEK<br><br>128 bit value | CTR-DRBG | NVRAM | Created when CO changes PIN/Password |
| | | | | Destroyed on PIN/Password change, zeroization |
| XTS-AES DEK | Encryption and decryption of user data<br><br>XTS-AES 256 bit key | CTR-DRBG | RAM | Created when first PIN/Password, either User or CO, is set |
| | | | | Destroyed on lock, timeout, entering low-power mode, power-off, and zeroization |
| User KEK | Obfuscation and unobfuscation of DEK<br><br>SIV AES 128 bit key | User PIN/Password, User Salt, and PBKDFv2 | RAM | Created before obfuscating) or unobfuscating the DEK. |
| | | | | Destroyed immediately after use |
| CO KEK | Obfuscation and unobfuscation of DEK<br><br>SIV AES 128 bit key | CO PIN/Password, CO Salt, and PBKDFv2 | RAM | Created before obfuscating or unobfuscating the DEK. |
| | | | | Destroyed immediately after use |

*Table 10: Critical Security Parameters*

## 6.3 Zeroization of Critical Security Parameters

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle to zeroize CSPs stored in NVRAM. Copies of CSPs in RAM are erased by setting the memory to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User CSPs. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User PIN/Password. However, if there is no CO PIN/Password, the user data partition will be erased leaving the module in the factory reset state with an erased use data partition.

The second kind of brute-force attack is against the CO PIN/Password. Ten consecutive failed attempts to unlock the module as CO will zeroize all CSPs for both the CO and User rôles, including the DEK. The module will be left in the factory reset state with an erased user data partition.

### 6.3.1 Zeroization via Factory Reset

A Factory Reset will erase all CSPs, settings, and user data from the module. After this operation, the operator must initialize the module per section 3.2 to return it to a FIPS approved mode.

Starting with the module disconnected from a USB port,

1. Press and hold the **7** button. Press and release the **KEY** button. Release the **7** button. The red and green LEDs will alternate. If the LEDs do not illuminate, connect the module to a USB power source and charge the battery for at least one minute. Disconnect the module from USB and restart this procedure.
2. Enter the sequence **999**. The red and green LEDs will continue to alternate.
3. Press and hold the **7** button. Press and release the **KEY** button. Release the **7** button. If the procedure is correctly performed, the red and green LEDs will illuminate together while the module erases
4. On completion, the LEDs turn off.

# 7 EMI/EMC Regulatory Compliance

This module conforms to the EMI/EMC requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

# 8 Self-Tests

When the module powers on, it performs a sequence of self-tests. If any of these tests fails, the drive will enter an error state. The module cannot perform any cryptographic services and is not usable in this state. The module also performs continuous self-tests. The only way to clear a module error state is to cycle the power. Self-tests are summarized in Table 11.

| Test Category | Test Name | When Executed | Failure Indications |
|---|---|---|---|
| Firmware Integrity | Firmware CRC-32 | Module power-on | Module illuminates no LEDs and does not respond to button presses. |
| | Firmware CRC-16 | Module power-on | Module fails to mount to host PC after successful unlock and returns to locked state. |
| Known Answer | DRBG Cert. #C 78 KAT[20]s<br>CTR-DRBG Instantiate<br>CTR-DRBG Generate | Module power-on | LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily. |
| | PBKDFv2 combined KATs<br>HMAC SHA-1 Cert. #C 78<br>SHA-1 Cert. #C 78 | Module power-on | LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily. |
| | AES #C 78 KATs<br>AES ECB encrypt Cert. #C 78<br>AES ECB decrypt Cert. #C 78<br>AES CMAC Cert. #C 78 | Module power-on | LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily. |
| | XTS-AES Cert. #AES 5942 KATs<br>AES-XTS encrypt<br>AES-XTS decrypt | Module power-on | Module fails to mount to host PC after successful unlock. Module automatically locks and illuminates red LED. |
| Conditional | NDRNG Conditional Test | Use of NDRNG | LEDs illuminate two times in circling pattern, red then green then blue. Red LED illuminates, fades out, and then red illuminates steadily. |
| | AES-XTS Cert. #AES 5942 Conditional<br>FIPS 140-2 IG A.9 AES-XTS Key Generation Test | Creation of DEK | Module fails to mount to host PC after successful unlock. Module automatically locks and illuminates red LED. |

*Table 11: Module Self-Tests*

20 KATs are Health tests per section 11.3 of SP800-90A. The CRNGT per section 4.9.2 of FIPS 140-2 is not necessary per IG 9.8.

# 9 Mitigation of Other Attacks

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

# 10 Glossary of Terms and Acronyms

| Term | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| CO | Cryptographic Officer |
| CRC | Cyclic Redundancy Check |
| CSP | Critical Security Parameter |
| CTR-DRBG | Counter-Mode Deterministic Random Byte Generator |
| DEK | Data Encryption Key |
| DRBG | Deterministic Random Byte Generator |
| ECB | Electronic Code Book |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Protocol |
| HMAC | Keyed-Hash Message Authentication Code |
| KAT | Known Answer Test |
| KEK | Key Encryption Key |
| LED | Light Emitting Diode |
| NDRNG | Non-deterministic Random Number Generator; module entropy source |
| NIST | National Institute of Standards and Technology |
| NVRAM | Non-volatile Random Access Memory |
| PBKDFv2 | Password Based Key Derivation Algorithm Version 2 |
| PIN | Personal Identification Number; synonym for password |
| RAM | Random Access Memory |
| Salt | Random value used to improve security of cryptographic algorithms |
| SATA | Serial AT Attachment |
| SHA-1 | Secure Hash Algorithm 1 |
| SHS | Secure Hash Standard |

| | |
|---|---|
| SIV | Synthetic Initialization Vector |
| USB | Universal Serial Bus |
| XTS-AES | AES cipher mode used to encrypt user data in mass storage |
| Zeroization | The process of erasing cryptographic security keys and parameters |